University of Chicago Legal Forum

Volume 1996 | Issue 1 Article 17

Entrapment in Cyberspace: A Renewed Call for Reasonable Suspicion

Jarrod S. Hanson
Jarrod.Hanson@chicagounbound.edu

Follow this and additional works at: http://chicagounbound.uchicago.edu/uclf

Recommended Citation
Hanson, Jarrod S. () "Entrapment in Cyberspace: A Renewed Call for Reasonable Suspicion," *University of Chicago Legal Forum*: Vol. 1996: Iss. 1, Article 17.
Available at: http://chicagounbound.uchicago.edu/uclf/vol1996/iss1/17

This Comment is brought to you for free and open access by Chicago Unbound. It has been accepted for inclusion in University of Chicago Legal Forum by an authorized administrator of Chicago Unbound. For more information, please contact unbound@law.uchicago.edu.

Entrapment in Cyberspace: A Renewed Call for Reasonable Suspicion

Jarrod S. Hanson†

DRoach, as the man identified himself, began a relationship with a thirteen-year-old girl on a computer chat group.[1] In time, DRoach's messages began to discuss sex. Soon, pictures accompanied his words.[2] Through these messages and pictures, DRoach made his sexual interest in his prospective victim clear.[3] He eventually asked the girl to meet him discreetly and to bring money to help pay for a motel room for their use.[4] When he arrived at the meeting point, he did not find a thirteen-year-old girl.[5] Instead, he found the police waiting to charge him with attempted carnal intercourse with a minor, attempted lewd and lascivious acts with a minor, and twenty-three counts of promoting or possessing child pornography.[6] The thirteen-year-old girl was actually a thirty-three-year-old law enforcement agent.[7]

This incident illustrates two dangers. First, it demonstrates that cyberspace provides a new forum for criminal activity. Child pornography and sex crimes are two of many crimes that people can commit online. Fraud, theft, libel, and consensual crimes, such as pornography and trafficking in illegal information, have also found their way into cyberspace.[8] Second, the DRoach incident illustrates the potential for overzealous law enforcement in cyberspace. Police officers,[9] service providers,[10] and private

---

† B.A. 1994, University of Denver; J.D. Candidate 1997, University of Chicago.

[1] Monica Davey, *Vice Squad Sleuths the Internet*, St. Petersburg Times 1B (Aug 13, 1995).

[2] Id.

[3] Id.

[4] Id.

[5] Davey, St. Petersburg Times at 5B (cited in note 1).

[6] Id.

[7] Id.

[8] See Edward A. Cavazos and Gavino Morin, *Cyberspace and the Law: Your Rights and Duties in the Online World* 78, 89, 107, 117-18 (MIT Press, 1994).

[9] See Jan Vertefeuille, *Hypersting Net Draws in Local Man*, Roanoke Times A1 (Sept 27, 1995) (describing a bulletin board law enforcement officials have set up to catch people stealing credit card numbers and cellular phone account numbers).

[10] See Davey, St. Petersburg Times at 5B (cited in note 1).

individuals[11] are eager to combat crime in cyberspace and can be creative in their efforts to do so.

The ease with which law enforcement officials can assume false identities in cyberspace and the suitability of cyberspace for consensual or victimless crimes indicate a probable increase in undercover sting operations. Defendants are therefore likely to invoke the entrapment defense with increasing frequency.

In light of the new stress placed on entrapment, courts will need to revisit the defense to determine whether it will serve its original purposes when applied to cyberspace. This Comment argues that the current entrapment doctrines as applied to cyberspace do not effectively address the concerns behind the entrapment defense. It argues that requiring law enforcement to meet a reasonable-suspicion standard before engaging in undercover operations would better address those concerns. Many commentators have called for the application of a reasonable-suspicion standard outside cyberspace.[12] This Comment renews their call for a reasonable-suspicion standard in all undercover operations by illustrating how such a standard would be more effective in cyberspace than the current entrapment test. Part I outlines the origins of the two tests for the entrapment defense in the federal courts and argues that both tests are striving for the same two goals. Part II illustrates how neither of the two court-created tests accomplishes the dual goals of limiting police activity and protecting the innocent when applied to situations in cyberspace. Finally, Part III argues that a reasonable-suspicion standard for police conduct would best accomplish the entrapment defense's policy goals in cyberspace.

---

[11] See Peter H. Lewis, *Nevada Man Finds FBI Waiting after Setting up Internet Tryst*, San Francisco Chronicle A6 (July 14, 1995) (describing a private investigator who posed as a fourteen-year-old girl on the Internet and provided information to law enforcement officers when a man asked to meet her to have sex).

[12] See Comment, *Lead Us Not into (Unwarranted) Temptation: A Proposal to Replace the Entrapment Defense with a Reasonable-Suspicion Requirement*, 133 U Pa L Rev 1193, 1216 (1985); Note, *The Government as Pornographer: Government Sting Operations and Entrapment:* United States v. Jacobson *916 F.2d 467 (8th Cir. 1990), rev'd, 112 S.Ct. 1535 (1992)*, 61 U Cin L Rev 1067, 1088-94 (1993); Comment, *If the Postman Always "Stings" Twice, Who Is the Next Target?—An Examination of the Entrapment Theory*, 19 J Contemp L 217, 244 (1993); Note, United States v. Jacobson: *A Call for Reasonable Suspicion of Criminal Activity as a Threshold Limitation on Governmental Sting Operations*, 44 Ark L Rev 493, 510 (1991).

I. THE DEVELOPMENT OF THE ENTRAPMENT DEFENSE

Courts have long recognized the need for police to use deception to catch criminals.[13] They have also recognized the potential dangers of such a practice.[14] The entrapment defense responds to these concerns about police involvement in undercover activities.

The Supreme Court has developed two tests, the subjective and objective tests, to examine the propriety of undercover police activities.[15] Both tests seek to advance the same policy objectives: preventing the abuse of police authority and protecting the "otherwise innocent"—those people who would be innocent of wrongdoing absent police inducement.[16]

A. The Subjective Test for Entrapment

The Supreme Court first announced the entrapment defense in *Sorrells v United States*.[17] In *Sorrells*, a government agent went undercover to investigate violations of the National Prohibition Act.[18] Three of Sorrells's acquaintances introduced him to the agent.[19] The agent and one of the acquaintances discovered that they had served in the same military division during World War I.[20] While they reminisced about the war, the agent asked Sorrells three times for some liquor, hoping to catch Sorrells in violation of laws prohibiting the possession of liquor.[21] Upon the third request, Sorrells produced a half gallon of liquor.[22]

While eight Supreme Court Justices agreed that Sorrells should have the defense of entrapment,[23] they divided sharply

---

[13] See *Sorrells v United States*, 287 US 435, 441 (1932) (stating that "[a]rtifice and stratagem may be employed to catch those engaged in criminal enterprises"); *United States v Russell*, 411 US 423, 436 (1973) (stating that "there are circumstances when the use of deceit is the only practicable law enforcement technique available").

[14] See *Sorrells*, 287 US at 442 (recognizing that difficulties arise "when the criminal design originates with the officials of the Government, and they implant in the mind of an innocent person the disposition to commit the alleged offense and induce its commission in order that they may prosecute").

[15] See notes 17-52 and accompanying text.

[16] Jonathan C. Carlson, *The Act Requirement and the Foundations of the Entrapment Defense*, 73 Va L Rev 1011, 1032 (1987).

[17] 287 US 435 (1932).

[18] Id at 439.

[19] Id.

[20] Id.

[21] *Sorrells*, 287 US at 439.

[22] Id.

[23] Justice McReynolds would have affirmed the lower court's decision to deny Sorrells the entrapment defense. Id at 453.

over both the proper test for entrapment and the theoretical underpinnings of the defense.[24] Chief Justice Hughes delivered the Court's opinion and set forth what would become the subjective test for entrapment. His opinion focused on determining who instigated the criminal design.[25] By focusing on the origin of the criminal plan, Chief Justice Hughes invited scrutiny of the defendant's character and predisposition. His concern was that police action not lead "otherwise innocent" people to commit crimes,[26] and he believed that an examination of the "predisposition and criminal design of the defendant" would shed light on whether the accused was in fact "otherwise innocent."[27]

The Court revisited entrapment in *Sherman v United States*.[28] A five-justice majority confirmed the subjective test as the law.[29] Chief Justice Warren's opinion again highlighted the doctrine's goal of protecting the innocent. He exhibited this concern through his statement that "Congress could not have intended that its statutes were to be enforced by tempting innocent persons into violations."[30] By depicting those ensnared by these police tactics as innocent, he showed his reliance on the predisposition criterion to ensure that those who are "otherwise innocent" receive the defense.

The Court explored other aspects of the entrapment defense in later decisions, but the majority opinions have continued to apply the subjective test.[31] The latest Supreme Court decision involving the entrapment defense is *Jacobson v United States*.[32] In *Jacobson*, the Court further defined the predisposition requirement while continuing to show concern for both goals of the entrapment defense.

Jacobson concerned a government mail sting to catch purchasers of child pornography.[33] As part of this operation, the government began sending surveys regarding sexual interests to

---

[24] See notes 25-27 and notes 42-45 and accompanying text.

[25] *Sorrells*, 287 US at 441.

[26] Id at 448.

[27] Id at 451.

[28] 356 US 369 (1958).

[29] Id. A four-justice concurrence supported the objective test. See notes 47-49 and accompanying text.

[30] Id at 372.

[31] See *Russell*, 411 US at 433; *Hampton v United States*, 425 US 484, 490 (1976); *Mathews v United States*, 485 US 58, 63 (1988).

[32] 503 US 540 (1992).

[33] Id at 542-47.

Keith Jacobson, a farmer in Nebraska.[34] He was the target of the operation because he had ordered some material oriented toward child pornography at a time when it was legal to order such material.[35] He also responded to some of the government's surveys.[36] After twenty-six months of repeated attempts by the government to induce Jacobson to violate the child pornography law, he ordered some pornographic material and was convicted.[37] The Supreme Court, however, concluded that the government entrapped him.[38]

The Court's analysis focused on the predisposition question. The majority found that the government had not proven that Jacobson's predisposition to order pornography "was independent and not the product of the attention that the Government had directed at petitioner."[39] The majority, through its examination of predisposition, evidenced its concern for ensuring the government's actions do not entrap the innocent. It concluded that a rational juror could not find that Jacobson's predisposition to commit crime "existed independent of the Government's many and varied approaches to [Jacobson]."[40]

B. The Objective Test for Entrapment

Although the Court has always applied the subjective test, a history of vigorous minority endorsement of the objective test exists.[41] The objective test has a different focus and illustrates the other goal of entrapment—to control law enforcement behavior.

Justice Roberts's concurring opinion in *Sorrells* set forth the objective test.[42] The objective test emerges from his differing view about the fundamental justification for the entrapment defense. Justice Roberts advocated the entrapment defense to protect the integrity of the judicial system rather than to effectuate the intent of Congress.[43] For this reason, he did not under-

---

[34] Id at 542, 544.

[35] Id at 542-43.

[36] *Jacobson*, 503 US at 543-44.

[37] Id at 546-47.

[38] Id at 542.

[39] Id at 550.

[40] *Jacobson*, 503 US at 553.

[41] The following dissenting and concurring opinions used the objective test: *Sorrells*, 287 US at 458-59 (Roberts concurring); *Sherman*, 356 US at 382-83 (Frankfurter concurring); *Russell*, 411 US at 436-37 (Douglas dissenting); *Russell*, 411 US at 439 (Stewart dissenting); and *Hampton*, 425 US at 496-97 (Brennan dissenting).

[42] *Sorrells*, 287 US at 458-59 (Roberts concurring).

[43] Id at 457 (Roberts concurring).

take to evaluate the predisposition or character of the defendant.[44] Rather, he focused exclusively on the actions of the government.[45]

Under the objective test, the jury scrutinizes the conduct of law enforcement. By focusing on the actions of the government, the jury provides a check on law enforcement. The nature of the government's action determines whether upholding a conviction would be a "prostitution of the criminal law."[46] Therefore, the government must ensure that its actions do not constitute entrapment.

The objective test again found support when Justice Frankfurter wrote a concurring opinion in *Sherman* urging the Court to adopt the objective test.[47] He set forth the objective test by stating that

> in holding out inducements [law enforcement agents] should act in such a manner as is likely to induce to the commission of crime only [those engaged in criminal conduct and ready and willing to commit further crimes should the occasion arise] and not others who would normally avoid crime and through self-struggle resist ordinary temptations.[48]

This formulation effectively eliminates consideration of a person's predisposition to commit a crime and instead focuses on police behavior and its effects on ordinary people.

Justice Frankfurter disagreed with the majority about the appropriate test for entrapment, but his adoption of the objective test shows his concern for controlling law enforcement behavior. He exhibits this concern in the following statement: "The courts refuse to convict an entrapped defendant, not because his conduct falls outside the proscription of the statute, but because, even if his guilt be admitted, the methods employed on behalf of the Government to bring about conviction cannot be countenanced."[49]

The objective test appears to have died at the federal level in the *Jacobson* decision, as neither the majority nor the minority embraced its use.[50] Many states[51] and the Model Penal Code,[52]

---

[44] Id at 458 (Roberts concurring).

[45] Id at 459 (Roberts concurring).

[46] *Sorrells*, 287 US at 457 (Roberts concurring).

[47] *Sherman*, 356 US at 382-83 (Frankfurter concurring).

[48] Id at 383-84 (Frankfurter concurring).

[49] Id at 380 (Frankfurter concurring).

[50] See 503 US 540. Although Justice Brennan filed a concurring opinion in *Mathews*,

however, have adopted the objective test for the reasons presented above. This Comment will therefore evaluate the effectiveness of both the subjective and objective tests as applied to undercover activities in cyberspace.

II. NEITHER THE SUBJECTIVE NOR THE OBJECTIVE TEST EFFECTUATES THE TWO PURPOSES OF ENTRAPMENT WHEN APPLIED IN CYBERSPACE

A. The Subjective Test Will Not Protect the Innocent in Cyberspace

The subjective test seeks to protect innocent defendants by examining a defendant's predisposition—defined as "how the defendant likely would have reacted to an *ordinary* opportunity to commit the crime."[53] While this test may protect defendants who were not predisposed, it fails to prevent the harmful side effects of a sting operation.

Being the target of a sting may provoke an individual to reveal more about himself to the government than he otherwise would. Child-pornography stings show this potential side effect of undercover operations. At the beginning of some of these operations, the government sent out questionnaires to individuals asking them to respond to a variety of inquiries.[54] Often the government took the individuals' names off mailing lists of pornography operations that the government had recently investigated.[55]

---

485 US at 66 (Brennan concurring), stating that he was bowing to stare decisis and accepting the subjective test, id at 67 (Brennan concurring), the case did not directly concern the application of the entrapment defense. *Jacobson* therefore marks the first time that the test for entrapment was squarely on the table and all the Justices used the subjective test.

[51] See Alaska Stat § 11.81.450 (1995); Ark Stat Ann § 5-2-209 (1993); 1986 Colo Rev Stat § 18-1-709; Fla Stat Ann § 777.201 (West 1992); Hawaii Rev Stat § 702-237(1) (1985); NJ Stat Ann § 2C:2-12a (West 1995); ND Cent Code § 12.1-05-11 (1985 and Supp 1995); 18 Pa Cons Stat Ann § 313(a) (Purdon 1983); Tex Penal Code Ann § 8.06(a) (Vernon 1994); and Utah Code Ann § 76-2-303(1) (1995).

[52] Model Penal Code § 2.13(1) (ALI 1962).

[53] *United States v Gendron*, 18 F3d 955, 962 (1st Cir 1994). The opinion in *Gendron* contains now-Justice Breyer's influential post-*Jacobson* formulation of the predisposition test.

[54] For example, in *United States v Mitchell*, 915 F2d 521, (9th Cir 1990), the government sent a ten-part application asking the applicants to "express their attitudes toward a broad spectrum of sexual and non-sexual activities." Id at 523. See also *United States v Byrd*, 31 F3d 1329, 1331 (5th Cir 1994); *United States v Chin*, 934 F2d 393, 395 (2d Cir 1991).

[55] In *Mitchell*, 915 F2d 521, for example, the government used records containing thousands of names which law enforcement agents seized pursuant to the arrest of a

The responses to these questionnaires narrowed the number of people the sting continued to target.[56] Although the effort seemed laudable, the result was that many people unwittingly revealed deeply personal information about themselves to public officials.

The court noted that targeted individuals who are not predisposed will simply ignore the solicitation or questionnaire.[57] This claim, however, is not true in all instances. Some of the questionnaires are "designed to attract the interest of individuals possessing . . . a broad range of legal sexual and non-sexual interests."[58] Because these operations cover many types of people and ask about a broad range of issues, many non-predisposed people may involuntarily reveal very private interests to the police.

The environment of cyberspace magnifies this problem. Law enforcement officials in cyberspace might not face the same economic constraints, such as printing and mailing costs, that force them to use care in selecting targets outside cyberspace. The costs of using a computer to distribute materials for testing and identifying potential targets would be much lower than the use of print material or human agents. The innocent in cyberspace receive less protection from being the target of undercover operations under the subjective test.

B. The Subjective Test Will Not Control Law Enforcement Officials in Cyberspace

In cyberspace, the subjective test for entrapment will exert little control over police behavior. Child pornography stings often select their targets from confiscated lists.[59] Cyberspace allows the generation of many more lists because of the high volume of transactions recorded on computers that can sort the information in various ways to create profiles of certain types of people.[60]

---

woman who purportedly controlled eighty percent of the United States market for child pornography. Id at 525 n 5.

[56] In *Mitchell*, 915 F2d 521, the defendant was one of "thousands" to whom the government sent a questionnaire. Id at 424-25. Law enforcement agents used responses to the questionnaire to narrow the list to 1400 targets. Id at 525.

[57] The court in *United States v Stanton*, 973 F2d 608 (8th Cir 1992), made a point of mentioning that the defendant "did not ignore the questionnaire or check a line at the top of the questionnaire indicating he was disinterested [sic] and wished to be removed from the mailing list." Id at 609.

[58] *Mitchell*, 915 F2d at 524 n 4.

[59] See notes 54-56 and accompanying text.

[60] A common example of such sorting is a supermarket with a system that scans the customer's identity from a card before recording his purchases. The store receives a profile

Although law enforcement has only limited access to transactional data accumulated by businesses,[61] it might be able to use its own means to gather information about potential targets. One author contends that the FBI maintained a program with librarians to identify suspicious users of sensitive, unclassified material who might conceivably represent a threat to the competitive or security status of the United States.[62] Cyberspace makes possible a more detailed accumulation of information about people the government deems suspicious or dangerous. Currently, "'companies can [ ] track trails of "mouse droppings" over the Internet, finding out which Web sites you go to and for how long.'"[63]

Law enforcement might use information of this nature to prove predisposition before government contact. If the use of such information is accepted, law enforcement actions will be unrestrained as courts will not place their activities under scrutiny.

Outside cyberspace, courts would occasionally scrutinize the government's actions in an undercover operation when examining predisposition. In *Jacobson v United States* and *United States v Gifford*, the courts looked at the contact the government had with the individual to determine whether it contributed to the person's disposition toward committing the crime.[64] In this way, the courts checked the types of operations conducted by the government. If the government, however, may prove predisposition as or before any contact occurs, courts will have no reason to examine the nature of the government's contact, significantly reducing the check on law enforcement behavior.

---

of purchases by the individual and uses that profile to make predictions about what products might appeal to that customer. For an in-depth analysis of this type of activity, see Oscar H. Gandy, Jr., *The Panoptic Sort: A Political Economy of Personal Information* (Westview Press, 1993).

[61] The Stored Wire and Electronic Communications and Transactional Records Access Act, 18 USC §§ 2701 et seq (1994), requires that law enforcement agents have authorization before accessing the transactional data of a business. 18 USC at § 2703.

[62] Herbert N. Foerstel, *Surveillance in the Stacks: The FBI's Library Awareness Program* (Greenwood Press, 1991).

[63] Vic Sussman and Kenan Pollack, *Gold Rush in Cyberspace*, US News and World Report 72, 78 (Nov 13, 1995) (quoting Larry Irving, Administrator of the National Telecommunications and Information Administration).

[64] *Jacobson v United States*, 503 US 540, 550-553 (1992); *United States v Gifford*, 17 F3d 462, 468 (1st Cir 1994).

C. The Objective Test Will Not Protect the Innocent in Cyberspace

The objective test does no better than the subjective test in protecting the innocent in cyberspace. The objective test examines the inducement offered by the government and evaluates its effects on the ordinary or hypothetical person.[65] If the ordinary person would commit the crime, the government has overreached, and the defendant may raise the entrapment defense.

Defining the hypothetical "ordinary person" in cyberspace will be difficult. One critic of the objective test applied outside cyberspace questioned how one can measure the fortitude of the average law-abiding citizen.[66] Not only is determining who represents the average citizen difficult, determining the level of resistance society expects beyond the standards in criminal laws is also difficult.

Cyberspace shares these difficulties and presents even greater ones. In examining the effect of police behavior on the hypothetical person, the court and jury assess the reasonableness of a law enforcement officer's activity. Such assessments of reasonableness are more difficult in cyberspace because the jury "may not know and may have no basis for knowing what is reasonable in cyberspace."[67]

Although one commentator claims that tests involving a hypothetical or "reasonable" person could translate into cyberspace,[68] these tests also have problems. Decisions about what is reasonable depend on the members of the jury, and their assessments of what is reasonable depend on their experiences.[69] Courts might, however, compensate for their lack of experience in cyberspace through expert witnesses and other testimony concerning Internet practices and mores.[70]

Consider the following scenario regarding how the objective test provides less protection for the innocent in cyberspace than outside cyberspace. Imagine that law enforcement agents who are

---

[65] See notes 42-52 and accompanying text.

[66] Comment, *Lead Us Not into (Unwarranted) Temptation: A Proposal to Replace the Entrapment Defense with a Reasonable-Suspicion Requirement*, 133 U Pa L Rev 1193, 1212 (1985).

[67] I. Trotter Hardy, *The Proper Legal Regime for "Cyberspace"*, 55 U Pitt L Rev 993, 1013 (1994).

[68] Id.

[69] See id at 1014.

[70] See id at 1040-41 (discussing the use of custom to influence decisions concerning reasonableness in cyberspace).

hoping to catch software pirates place some copyrighted material on the Internet and make it easy to download. The material also contains some warnings about its copyrighted status. Upon discovering this material, a user does not read the warnings because much of what he has come across on the Internet has some introduction, instruction, or advertisement; and he has found that most of the time they are unimportant and unhelpful. He downloads the information. At his trial, he raises the entrapment defense. Many difficult questions arise. For example, was the offered software unusually attractive compared to what might otherwise be available? How much of the material in similar settings would be illegal to download? Was the warning adequate compared to others on the Internet? Would most copyrighted information made available have a warning so that a person would know whether to be concerned?

These questions, among others, might influence a fact-finder's decision about the effect of the government's action on an ordinary person. Resolving them in court might mean that defendants bear a great financial burden to provide expert witnesses. Even if the person is found innocent, he will not have been shielded from a long and expensive process.

D. The Objective Test Will Not Control Law Enforcement in Cyberspace

The objective test, although designed to limit law enforcement behavior, will do little to control law enforcement behavior in cyberspace. The effectiveness of the test in controlling law enforcement behavior depends in part on the court's issuing guidelines to which the police can conform their behavior.[71] No current cases apply the entrapment defense in cyberspace, leaving law enforcement without guidelines. Although this problem may diminish as courts make decisions concerning entrapment in cyberspace, no guidelines currently exist for police behavior.[72]

One possible solution would be to translate the guidelines from the non-cyberspace objective standard to situations in cyberspace. Many of these standards, however, do not translate. For example, fostering sexual relationships to encourage crime is

---

[71] See Roger Park, *The Entrapment Controversy*, 60 Minn L Rev 163, 225 (1976).

[72] Another problem which might arise is that the guidelines developed for entrapment might not be objective but instead might be the result of public pressure to stop crime at any cost. The stringency of the guidelines might vary directly with the public's estimate of the seriousness of crime in cyberspace.

generally outside the range of acceptable law enforcement behavior in the real world.[73] In cyberspace, sex is not possible in the conventional sense. Would the offer of sexual favors be off limits in cyberspace without a real chance of them occurring? If an agent through words satisfies someone's desires, is such conduct also off limits even though no physical contact occurred? Although courts might eventually answer these questions, law enforcement activity will proceed unguided until that point.

Similarly, the courts have consistently said that beseechments to commit crime based primarily on "sympathy, pity, or close personal friendship" likely constitute prohibited activity under the objective test.[74] Such a standard provides little concrete guidance outside cyberspace and would provide even less guidance if imported into cyberspace. For example, uncertainty remains about whether correspondence with people on a drug recovery bulletin board about getting drugs to ease withdrawal would constitute an unacceptable play on sympathy. Also, from whose perspective will the jury or judge examine whether a close personal friendship existed—from the point of view of the officer who was, in his mind, simply carrying on a series of conversations, or from the point of view of someone whose only conversational interaction with other people was over the computer? The second person might have felt that anyone willing to spend time communicating with her was a close friend for whom she would do anything, including commit a crime. If this situation were to occur outside cyberspace, the defendant would have encountered the undercover agent, and she would receive more clues about the nature of the relationship from face-to-face contact. In cyberspace, these clues are reduced. Interactions occurring in cyberspace give law enforcement the potential to have greater influence over a person while staying within the boundaries of current guidelines. The number of cues given to a target is reduced. The result is that police conduct will not be deterred

---

[73] Several courts have disapproved of officers fostering relationships with sexual overtones and then exploiting them to induce a person to commit crime. See *Commonwealth v Thompson*, 335 Pa Super 332, 484 A2d 159, 166 (1984) (finding entrapment as a matter of law where law enforcement used "a young, blonde female to coax a middle age [sic] male, after months of kissing and socializing, into committing a minor crime"); *People v Wisneski*, 96 Mich App 299, 292 NW2d 196, 199 (1980) (stating that "[p]olice encouragement of an agent's use of sex to induce one who is unwilling and unready to commit a crime constitutes entrapment").

[74] See, for example, *Grossman v State*, 457 P2d 226, 230 (Alaska 1969); *State v Mullen*, 216 NW2d 375, 383 (Iowa 1974); *State v Taylor*, 599 P2d 496, 503 (Utah 1979).

in these situations by applying the standards generated from the application of the objective test in the real world.

III. A REASONABLE-SUSPICION STANDARD EFFECTIVELY ADDRESSES THE PROBLEMS OF THE ENTRAPMENT DEFENSE IN CYBERSPACE

Legislatures and courts should replace the entrapment defense with a requirement that law enforcement officials prove a reasonable suspicion that the target of an undercover operation has engaged in or is likely to engage in criminal activity. They should also have to show that an undercover operation is related to the suspected illegal activity of the target and that the scope of their operation is limited to its object.

Some members of the Supreme Court have not responded favorably to arguments for a reasonable-suspicion standard. In *Jacobson*, Justice O'Connor's dissent accused the majority of imposing what she interpreted to be a reasonable-suspicion requirement on law enforcement.[75] Several lower courts have also shown disfavor toward adopting a reasonable-suspicion standard.[76]

The reasonable-suspicion standard, however, has found support outside the courts. Several commentators have endorsed it.[77] After the Abscam series of entrapment cases, Congress investigated the entrapment doctrine. Committees in both houses concluded that a reasonable-suspicion requirement was necessary.[78] Additionally, the Attorney General's own guidelines re-

---

[75] *Jacobson v United States*, 503 US 540, 556 (1992) (O'Connor dissenting).

[76] See *United States v Harvey*, 991 F2d 981, 990 (2d Cir 1993) (rejecting a reasonable-suspicion requirement and noting that the weight of authority rejects a constitutional requirement of reasonable basis or suspicion).

[77] See Comment, *Lead Us Not into (Unwarranted) Temptation: A Proposal to Replace the Entrapment Defense with a Reasonable-Suspicion Requirement*, 133 U Pa L Rev 1193, 1216 (1985); Note, *The Government as Pornographer: Government Sting Operations and Entrapment:* United States v. Jacobson, *916 F.2d 467 (8th Cir. 1990), rev'd, 112 S.Ct. 1535 (1992)*, 61 U Cin L Rev 1067, 1089 (1993); Note, *Executive Targeting of Congressmen as a Violation of the Arrest Clause*, 94 Yale L J 647, 667-68 (1985)(recommending a reasonable-suspicion standard for undercover operations targeting members of Congress); Comment, *If the Postman Always "Stings" Twice, Who Is the Next Target?—An Examination of the Entrapment Theory*, 19 J Contemp L 217, 244 (1993); Note, United States v. Jacobson: *A Call for Reasonable Suspicion of Criminal Activity as a Threshold Limitation on Governmental Sting Operations*, 44 Ark L Rev 493, 510 (1991).

[78] See FBI Undercover Operations, HR Rep No 98-267, 98th Cong, 2d Sess 84 (1984) ("House Report"); Final Report of the Select Committee to Study Undercover Activities of Components of the Department of Justice, S Rep No 97-682, 97th Cong, 2d Sess 1, 377-89 (1983) ("Senate Report").

quire a reasonable "indication" of illegal activites before the commencement of undercover operations.[79]

In the face of judicial reluctance to modify the entrapment standard, the proper body to change the entrapment standard is the legislature.[80] The Supreme Court in *United States v Russell* acknowledged that "Congress may address itself to the question [of entrapment] and adopt any substantive definition of the defense that it may find desirable."[81]

The House Subcommittee that investigated undercover operations after Abscam recommended legislation that would require law enforcement to meet a reasonable-suspicion standard and receive judicial authorization prior to engaging in undercover operations.[82] Senator Mathias introduced a bill addressing these concerns to the Senate floor shortly after the Abscam cases, but it died in the Judiciary Committee.[83] The greater problems with the entrapment defense in cyberspace should provide the impetus for Congress to revisit its earlier conclusions and act on them by passing legislation requiring prior judicial approval of undercover operations based on the reasonable-suspicion standard.

Under this requirement, law enforcement officers would have to seek judicial approval for an operation by showing that they had reason to believe that an individual had engaged or would engage in criminal activity. They would also have to outline the scope of the activity and the goals of their undercover operation. The request for authorization would describe the types of inducements the undercover operation would employ so the judge or magistrate could evaluate their appropriateness.

The reasonable-suspicion requirement would protect the innocent in cyberspace. It would resolve the problem of the subjective test—innocent people revealing more information to the government than they otherwise would—by limiting the scope of undercover operations. The government should not be able to cast a broad net hoping to catch a few criminals. Instead, operations would focus only on those who meet the reasonable-suspicion standard, thereby protecting a large number of innocent people from revealing private information.

---

[79] Department of Justice, Office of the Attorney General, The Attorney General's Guidelines on Criminal Investigations of Individuals and Organizations, reprinted in S Rep No 97-682, 97th Cong, 2d Sess 504, 507 (1983).

[80] See note 75 and accompanying text.

[81] *United States v Russell*, 411 US 423, 433 (1973).

[82] House Report at 84 (cited in note 78).

[83] Cong Index 14,187 and 20,505 (CCH 97th Cong Senate 1983-84).

Jacobson illustrates how the reasonable-suspicion requirement would protect the innocent. Jacobson's name came from the mailing list of a pornography operation.[84] In cyberspace, the government might get lists of names from records of computer activity. At the very least, a reasonable-suspicion standard would require an examination of the reliability of such lists. If the people running the undercover operation had known that the activity which placed Jacobson's name on the list was legal at the time he did it, perhaps they would not have targeted him.[85] A reasonable-suspicion standard will require the government to examine the legality of the activity that places peoples names on lists in cyberspace to ensure that the activities are ones that would raise a reasonable suspicion of illegal activity.

The reasonable-suspicion test would also address the problem that the objective test had with protecting the innocent.[86] The judge's focus would switch from the "hypothetical" or "ordinary" person to the appropriateness of the operation in light of its individual circumstances. Judges could thus account for the effects that the environment of cyberspace has on the appropriateness of the operation's activities.

The reasonable-suspicion test would act as a check on law enforcement conduct. The problem with the subjective test's ability to control law enforcement behavior in cyberspace is that the information collection and sorting ability that cyberspace provides makes predisposition an easy obstacle to clear. Under a reasonable-suspicion standard, judges would examine the reasons to target people before an operation began, thereby controlling law enforcement. The government would not be able to undertake operations to catch individuals without much evidence of predisposition, hoping that the court would later approve its actions to avoid the embarassment of letting someone involved in child pornography go free.

In the same way that judges analyze the scope of a search with regard to its object,[87] judges should analyze scope of an un-

---

[84] *Jacobson*, 503 US at 543.

[85] The magazine that Jacobson ordered from the company was not illegal at the time he ordered it, and there was no indication that he ordered material of a similar nature once it became illegal. *Jacobson*, 503 US at 551.

[86] See notes 65-70 and accompanying text.

[87] The scope of a warrant is limited by the requirement of particularity. When executing a warrant, police must identify the object and location of their search and justify it by providing information regarding probable cause. See Wayne R. LaFave, 2 *Search and Seizure: A Treatise on the Fourth Amendment* § 4.5 at 513 and § 4.10 at 653 (West, 3d ed 1996).

dercover operation to ensure that its activities are limited to those relevant to achieving its goals. Although not every detail of an undercover operation could be predicted, it could be described in general terms and authorization could be granted for a range of actions.[88] For example, in authorizing an operation, a judge could limit law enforcement to offering certain types of inducements which are not excessive,[89] in light of the peculiar circumstances of cyberspace. This type of scrutiny would provide law enforcement with the incentive to make the operation as narrow as possible while still catching the person suspected of wrongdoing.

A difficulty with the reasonable-suspicion requirement lies in determining who would decide whether there is reasonable suspicion and examine the scope of an undercover operation. The House Subcommittee and Senate Committee differed over who should authorize undercover operations based on reasonable suspicion. The House advocated authorization from the judicial branch[90] while the Senate proposed authorization by the executive branch.[91] Similarly, some commentators advocate judicial involvement,[92] while other sources strongly reject prior judicial approval.[93]

Requiring judicial approval would best protect the innocent and control law enforcement behavior. The House Subcommittee advocated judicial approval of undercover operations because agencies were not enforcing their internal guidelines in a meaningful way.[94] This determination is not surprising because a law enforcement agency has little incentive to police itself, and the head or review board of the agency has the authority to interpret the guidelines.[95] Although "reasonable suspicion" has a developed meaning in the judicial arena, the agency can interpret the

---

[88] But see Katherine Goldwasser, *After Abscam: An Examination of Congressional Proposals to Limit Targeting Discretion in Federal Undercover Investigations*, 36 Emory L J 75, 129-30 (1987).

[89] For example, the court could look at the factors delineated in *United States v Gendron*, 18 F3d 955, 961-62 (1st Cir 1994), to ensure that law enforcement's actions are not excessive.

[90] House Report at 83-84 (cited in note 78).

[91] Senate Report at 25 (cited in note 78).

[92] See, for example, Comment, 133 U Pa L Rev at 1217-19 (cited in note 77).

[93] See ABA Report of Section of Criminal Justice Regarding Undercover Operations (1987), reprinted in Paul Marcus, *The Entrapment Defense* § 12.27 at 678 (Michie, 1989).

[94] House Report at 84 (cited in note 78).

[95] See Gary T. Marx, *Undercover: Police Surveillance in America* 184 (University of California Press, 1988) (noting that a weakness of internal guidelines is that the agencies themselves interpret the guidelines).

term in a way that is favorable to its interests. Also, since the violation of an agency's internal guideline might not result in any penalty, even a rigorously defined standard of reasonable suspicion might have little or no deterrent effect on law enforcement behavior.[96]

The Senate Report raised a number of objections to judicial approval.[97] It noted that undercover operations are fast-moving, requiring quick decisions.[98] While internal enforcement of guidelines might result in quicker action, rapid internal review is unlikely to be more than a rubber stamp of field officers' decisions. The Report also raised institutional objections to judicial involvement. The Report showed concern that the judicial system will be placing a "pre-operation imprimatur" on undercover operations by making determinations about the scope of undercover operations which the judicial system would have to review.[99] However, the same result occurs when judges issue warrants which judges might review at a later stage. Additionally, the Report argued that a judicially administered standard would add to the congestion of the courts.[100] This argument may be true, but the additional protection of the innocent would outweigh any additional judicial burden.

CONCLUSION

The entrapment defense developed to prevent law enforcement officials from inducing the otherwise innocent to commit crimes and to prevent them from overreaching their authority. Neither of the tests developed for entrapment, however, adequately accomplishes these goals when applied in cyberspace. Replacing the entrapment defense with the requirement that law enforcement have reasonable suspicion before engaging in an undercover activity would ensure that the policies undergirding the entrapment defense translate in cyberspace. Such a standard, by requiring that law enforcement show that the target is likely to commit a crime, protects the innocent and allows courts to scrutinize law enforcement officials to ensure that they stay within the scope of their authority.

---

[96] Id.

[97] Senate Report at 387-89 (cited in note 78).

[98] Id at 388-89.

[99] Id at 389.

[100] Id at 389.